

Appl. No. 09/735,088
 Amdt. dated December 27, 2004
 Reply to Office action of October 1, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A ~~cryptographic system in a computer system, said cryptographic system comprising:~~

~~at least one server;~~

~~a database, said database comprising constructed and arranged to contain sensitive information data, said database and responsive to signals from one of said at least one said server;~~

~~enterprise credentials stored in said database;~~

~~a key repository process executing on one of said at least one said server, said key repository and having comprising at least one a master key used by, said at least one master key being constructed and arranged said key repository process to protect manage said data information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database, said key repository further constructed and arranged to access said enterprise credentials; and~~

~~at least one an application program executing on at least one of said at least one said server;~~

~~wherein said key repository process is enabled to record stores and retrieves authorization information maintained in said database, said authorization information these used to determine if said applications program that are is authorized to obtain access said data enterprise credentials; and~~

~~wherein said key repository process prevents access to said data by said application program if said application program is not authorized.~~

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

2. (Currently amended) A cryptographic computer system as in claim 1, wherein said key repository process uses said at least one master key to protects decrypt said data sensitive information in said database.
3. (Currently amended) A cryptographic computer system as in claim 1, wherein said repository process uses said at least one master key to provides privacy protection to encrypt said data sensitive information on said database.
4. (Currently amended) A cryptographic computer system as in claim 1, wherein said data sensitive information is comprises a public key.
5. (Currently amended) A cryptographic computer system as in claim 1, wherein said data sensitive information is comprises a secret.
6. (Currently amended) A cryptographic computer system as in claim 1, wherein said data sensitive information is comprises a private key.
7. (Currently amended) A cryptographic computer system as in claim 1, wherein said data sensitive information is comprises a symmetric key.
8. (Currently amended) A cryptographic computer system as in claim 1, wherein said data sensitive information is comprises a certification authority certificate.
9. (Currently amended) A cryptographic computer system as in claim 1, wherein said master keys are is maintained kept in physical memory.
10. (Currently amended) A cryptographic computer system as in claim 1, wherein said master keys are kept is maintained in non-swappable physical memory.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

11. (Currently amended) A ~~cryptographic computer~~ system as in claim 10, wherein said non-swappable physical memory is protected.

12. (Currently amended) A ~~cryptographic computer~~ system as in claim 1, wherein said master keys are ~~kept~~ maintained in virtual memory.

13. (Currently amended) A ~~cryptographic computer~~ system as in claim 1, wherein ~~said said master key key repository stores an integrity key, said integrity key constructed and arranged to ensure the integrity of said is used to decrypt sensitive information a public key on maintained in said database; and~~ wherein said public key is used to encrypt said data.

14. (Currently amended) A ~~cryptographic computer~~ system as in claim 13, wherein said key repository process further stores comprises a protection second master key, said ~~protection second master key constructed and arranged to protect said sensitive information on said database used to encrypt the public key.~~

15. (Cancelled).

16. (Currently amended) A ~~cryptographic computer~~ system in a computer system, said ~~cryptographic system comprising:~~

~~at least one server;~~

a database, ~~said database constructed and arranged to contain comprising sensitive information enterprise credentials,~~ said database responsive to signals from one of said at least one server;

~~sensitive secrets stored in said database;~~

~~an~~ at least one application process executing on said at least one server;

and

a key repository process executing on said at least one server, said key repository process having at least one master key, said at least one

Appl. No. 09/735,088
 Amdt. dated December 27, 2004
 Reply to Office action of October 1, 2004

~~master key being constructed and arranged used by said key repository process to manage protect said information enterprise credentials in said database;~~

~~wherein said key repository further constructed and arranged to store maintains in said database the identity of those said at least one application processes that are authorized to access said sensitive secrets enterprise credentials said key repository further constructed and arranged to permit access to said sensitive secrets by said at least one application; and~~

~~wherein if said at least one application process is authorized to access said enterprise credentials sensitive secrets, then said key repository process transmits said sensitive secrets enterprise credentials to said at least one application process.~~

17. (Currently amended) A computer cryptographic system as in claim 16, wherein said ~~at least one master key~~ protects said ~~sensitive information in said database~~ enterprise credentials from modification.

18. (Currently amended) A computer cryptographic system as in claim 16, wherein said ~~at least one master key~~ provides privacy protection to said sensitive information in said ~~database~~ enterprise credentials.

19. (Currently amended) A computer cryptographic system as in claim 16, wherein said ~~at least one of master key~~ protects said sensitive information in said ~~database~~ enterprise credentials from unauthorized deletion.

20. (Currently amended) A computer cryptographic system as in claim 16, wherein said ~~sensitive secret is~~ enterprise credentials comprise a public key.

21. (Currently amended) A computer cryptographic system as in claim 16, wherein said enterprise credentials comprise ~~sensitive secret is~~ a private key.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

22. (Currently amended) A computer cryptographic system as in claim 16, wherein said enterprise credentials comprise sensitive secret is a symmetric key.

23. (Currently amended) A computer cryptographic system as in claim 16, wherein said enterprise credentials comprise sensitive secret is a trust root.

24. (Currently amended) A computer cryptographic system as in claim 23, wherein said trust root is comprises a digital fingerprint.

25. (Currently amended) A computer cryptographic system as in claim 23, wherein said trust root comprises is a checksum.

26. (Currently amended) A computer cryptographic system as in claim 23, wherein said trust root comprises is a hash.

27. (Currently amended) A computer cryptographic system as in claim 23, wherein said trust root comprises is a cryptographic mechanism.

28. (Currently amended) A computer cryptographic system as in claim 16, wherein said keys are is kept in physical memory.

29. (Currently amended) A computer cryptographic system as in claim 16, wherein said keys are is kept in non-swappable physical memory.

30. (Currently amended) A computer cryptographic system as in claim 16, wherein said non-swappable physical memory is protected.

31. (Currently amended) A computer cryptographic system as in claim 16, wherein said keys are is kept in virtual memory.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

32. (Currently amended) A method of ~~authorizing access to sensitive secrets on a computer system, said computer system having a server, an application, a database on said server, sensitive secrets on said server, and a key repository having at least one master key to manage said sensitive secrets on said database, said method comprising the steps of:~~

- (a) storing authorization information and data in said a database, said authorization information and said data that is accessible by said a key repository process;
- (b) storing a master key in said database, said master key used by said key repository process to protect said data;
- (~~bc~~) querying said key repository process by said an application program for access to said sensitive secrets data;
- (~~cd~~) determining if said application program is authorized to access said sensitive secrets data by querying said authorization information in said database; and
- (~~de~~) if said application program is authorized to access said sensitive secrets data, then transmitting said sensitive secrets data from said key repository to said application program;

~~wherein said application can invoke cryptographic resources on said server.~~

33. (Currently amended) The method of claim 32, ~~said method further comprising, before said step b), directing said key repository process to recognize an instances of said application program before querying said key repository process.~~

34. (Currently amended) The method of claim 32, wherein said key repository process is constructed and arranged to record said authorization information in said database.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

35. (Currently amended) The method of claim 32, wherein ~~at the first of said~~
~~two-master keys~~ protects said ~~sensitive secrets~~data from modification.

36. (Currently amended) The method of claim 32, wherein ~~a the second of~~
~~said two-master keys~~ provides privacy protection of said ~~sensitive secrets~~data
~~on said database.~~

37. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said sensitive secrets is~~data comprises a public key.

38. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said sensitive secrets is~~data comprises a private key.

39. (Currently amended) The method of claim 32, wherein ~~at least one of said~~
~~sensitive secrets is~~data comprises a symmetric key.

40. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said sensitive secrets is~~data comprises a trust root.

41. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said sensitive secrets is~~data comprises a digital fingerprint.

42. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said data comprises sensitive secrets is~~ a digital signature.

43. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said data comprises sensitive secrets is~~ a digital certificate.

44. (Currently amended) The method of claim 32, wherein ~~at least one of~~
~~said data comprises sensitive secrets is~~ a checksum.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

45. (Currently amended) The method of claim 32, wherein ~~at least one of~~ said data comprises sensitive secrets is a hash.

46. (Currently amended) The method of claim 32, wherein ~~at least one of~~ said data comprises sensitive secrets is a characteristic code sequence.

47. (Currently amended) The method of claim 32, wherein said master keys are is kept in physical memory.

48. (Currently amended) The method of claim 32, wherein said master keys are is kept in non-swappable physical memory.

49. (Original) The method of claim 48, wherein said non-swappable memory is protected.

50. (Currently amended) The method of claim 32, wherein said master keys are is stored in virtual memory.

51. (Currently amended) The method of claim 32, wherein said ~~at least one~~ master key ~~is~~ comprises an Integrity key, said Integrity key being constructed and arranged to ensure the integrity of said ~~sensitive secrets on said~~ database data.

52. (Currently amended) The method of claim 32, wherein said ~~at least one~~ master key ~~is~~ comprises a protection key, said protection key being constructed and arranged to protect said ~~sensitive secrets on said~~ database data.

53. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by use of a cryptographic technique.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

54. (Original) The method of claim 53, wherein said cryptographic technique is a checksum.

55. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by its file location.

56. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by its physical address.

57. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by the system on which it is instantiated.

58. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by the nature of the interconnection to said key repository.

59. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by its communication protocol.

60. (Currently amended) The method of claim 33, wherein said instance of said application program is recognized by a packet header.

61. (Original) The method of claim 32, wherein said authorization information includes a time constraint.

62. (Original) The method of claim 32, wherein said authorization information includes a file location.

63. (Original) The method of claim 32, wherein said authorization information includes a physical address.

Appl. No. 09/735,088
Amdt. dated December 27, 2004
Reply to Office action of October 1, 2004

64. (Original) The method of claim 32, wherein said authorization information includes a universal resource locator.

65. (Original) The method of claim 32, wherein said authorization information includes a system residence.

66. (Currently amended) The method of claim 32, wherein ~~said directive to authorize~~storing said authorization information ~~said application is provided~~initiated by an operator.

67. (Currently amended) The method of claim 32, wherein ~~said directive to authorize~~storing said authorization information ~~said application is~~initiated~~provided~~ by an owner.

68. (Currently amended) The method of claim 32, wherein ~~said directive to authorize~~storing said authorization information ~~said application is~~initiated~~provided~~ by two or more owners.

69. (Currently amended) The method of claim 32, wherein ~~said directive to authorize~~storing said authorization information ~~said application is~~initiated~~provided~~ by two or more owners and an operator.